Amendments to the Specification

Pages 6-7. Amend the paragraph spanning these pages as follows:

Any data recorded in NAND record space 210 of memory 200 is transferred to record space 310 of receiving device 300. On this occasion, device authentication is performed between authentication section 232 of memory 200 and authentication section 320 of receiving device 300, and only if authentication is successful, data transfer is implemented from NAND record space 210 to record space 310. When reading data from memory 200, receiving device 300 performs authentication to authentication section 232 of memory 200 based on mutually common encryption function Hpc and nonpublic key Kpc specified by receiving device 300 so as to verify that it is the normal receiving device 300. In addition, as mentioned above, when transferring data to receiving device 300, memory 200 ensures with a built-in CPU that the image has not been changed since it was recorded by using data authentication algorithm Hcf and nonpublic key Kcf, and then transfers to receiving device 300 the data indicating that it is already ensured. It is possible to verify that the data is the data which came ~~trough~~ through a limited route from predetermined input device 100 based on authentication of memory 200 and information of "confirmation of no change" communicated from memory 200. The following shows a concrete process:

Page 9. In section 6, amend numbered paragraph 1 as follows:

1. For any attack on contents of a ROM in SDC and SCF, it is ~~taper resist~~ tamper resistant in which a code of a ROM cannot be analyzed from outside and contents of a ROM cannot be analyzed even if it is decomposed. Accordingly, the keys in it (Kdc, Kcf and Kx) cannot be attacked, either.